Verification of Declaration of Adherence | Update May 20th, 2021

Declaring Company: Alibaba Cloud (Singapore) Private Limited

Verification-ID	2020LVL02SCOPE013
Date of Upgrade	May 2021

Table of Contents

1 Need and Possibility to upgrade to v2.11, thus approved Code version

1.1 Original Verification against v2.6

The original Declaration of Adherence was against the *European Data Protection Code of Conduct for Cloud Service Providers* (**'EU Cloud CoC'**)[1] in its version 2.6 (**'v2.6'**)[2] as of March 2019. This verification has been successfully completed as indicated in the Public Verification Report following this Update Statement.

1.2 Approval of the Code and accreditation of the Monitoring Body

The EU Cloud CoC as of December 2020 (**'v2.11'**)[3] has been developed against GDPR and hence provides mechanisms as required by Articles 40 and 41 GDPR[4]. As indicated in 1.1. the services concerned passed the verification process by the Monitoring Body of the EU Cloud CoC, i.e., SCOPE Europe sprl/bvba[5] (**'SCOPE Europe'**). In alignment with the competent supervisory authority, SCOPE Europe has been applying the same rigorous procedures to verify Code compliance already prior the official approval of the Code and the Monitoring Body's accreditation.

May 2021, the Code has been officially approved as well as SCOPE Europe has been officially accredited as Monitoring Body.

1.3 Equality of Code requirements, anticipation of adaptions during prior assessment

SCOPE Europe followed each iteration of the Code carefully. At the time of this Declaration of Adherence, SCOPE Europe was already aware of updated versions of the Code and ensured that material differences, where applicable, were already addressed in its verification process.

SCOPE Europe could not identify material differences within each iteration since v2.6 that have significant influence on a CSP's Code adherence. Adaptions since v2.6 are either editorial or clarifying the Code's language that reflects the Monitoring Body's prior interpretation.

1.4 Equality of verification procedures

In accordance with the competent supervisory authority SCOPE Europe has been applying its procedures prior accreditation, already. This was intended to safeguard both the possibility to upgrade once

---

[1] https://eucoc.cloud
[2] https://eucoc.cloud/get-the-code
[3] https://eucoc.cloud/get-the-code
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679
[5] https://scope-europe.eu

the official approval and accreditation take place and to sufficiently test and verify the appropriateness and rigor of such procedures. Thus, following the accreditation procedures are not materially different than before. Adaptions requested during the process of accreditation were, as those requested to the Code, in general editorial or to clarify.

2 Conclusion of suitable upgrade on a case-by-case decision

Since the Code has been approved and the latest version of the Code has been published, SCOPE Europe as Monitoring Body has re-assessed its findings and documentation as provided by Alibaba Cloud.

SCOPE Europe concludes that there is no reason to doubt that Alibaba Cloud is compliant with v2.11 of the Code. Thus, the prior verification shall be upgraded to v2.11. Monitoring Body will further assess within Alibaba Cloud's renewal; alternatively, by its continuous pro-active monitoring, where deemed necessary.

3 Validity

This upgrade statement comprises of 4 pages. It is valid until the next official renewal of the upgraded Declaration of Adherence. This upgrade statement has been attached to the original Verification Report that follows this statement.

Original Verification-ID: 2020PV02SCOPE013

Upgraded Verification-ID: 2020LVL02SCOPE013

SCOPE EUROPE

Verification of Declaration of Adherence

Declaring Company: Alibaba Cloud, Declaring Services: IAAS

EU CLOUD COC

Verification-ID	2020PV02SCOPE013
Date of Approval	June 2020
Due date of Approval	June 2021

Table of Contents

1 Verification against v2.6 of the EU Cloud CoC

This Declaration of Adherence was against the *European Data Protection Code of Conduct for Cloud Service Providers* (**'EU Cloud CoC'**)[1] in its version 2.6 (**'v2.6'**)[2] as of March 2020.

Originally being drafted by the Cloud Select Industry Group[3] (**'C-SIG'**) the EU Cloud CoC, at that time being called C-SIG Code of Conduct on data protection for Cloud Service Providers, the Code was developed against Directive 95/46/EC[4] incorporates feedback by the European Commission as well as Working Party 29. Following an extensive revision of earlier versions of Code and further developing the substance of the Code v2.6 and its provisions has been aligned to the European General Data Protection Regulation (**'GDPR'**)[5].

The EU Cloud CoC already applies the same principles and procedures now, pending the endorsement of the Code and its official approval by supervisory authorities, cloud service providers are welcomed and invited to sign up their services under v2.6 of the EU Cloud CoC, to publicly underpin their efforts to comply with GDPR requirements.

2 List of declared services

2.1 Alibaba Cloud products and services

2.1.1 Elastic Computing

- Elastic Compute Service ("ECS")

2.1.2 Database Services

- Relational Database Service ("RDS")

2.1.3 Storage & CDN

- Object Storage Service ("OSS")
- Content Delivery Network ("CDN")

2.1.4 Networking

- Server Load Balancer ("SLB")

---

[1] https://eucoc.cloud
[2] https://eucoc.cloud/get-the-code
[3] https://ec.europa.eu/digital-single-market/en/cloud-select-industry-group-code-conduct
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046
[5] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679

- Virtual Private Cloud (“VPC”)

2.1.5 Security

- Alibaba Cloud Security

2.1.6 Networking

- Express Connect
- Elastic IP
- VPN Gateway
- NAT Gateway

2.1.7 Internet of Things

- Alibaba Cloud Link IoT Platform
- Alibaba Cloud Link Living
- Alibaba Cloud Link IoT Edge
- Alibaba Cloud Link ID²
- AliOS Things
- IoT Platform

2.1.8 Elastic Computing

- Simple Application Server
- Elastic GPU Service
- Auto Scaling
- Server Load Balancer
- Container Service
- Container Service for Kubernetes (ACK)
- Container Registry
- Resource Orchestration Service
- E-HPC
- ECS Bare Metal Instance
- Super Computing Cluster
- Function Compute
- Batch Compute
- Dedicated Host

2.1.9 Storage & CDN

- Table Store
- Network Attached Storage
- Hybrid Cloud Storage Array
- Data Transport
- Hybrid Backup Recovery
- Cloud Storage Gateway
- Dynamic Content Delivery Network (DCDN)

2.1.10 Networking

- Cloud Enterprise Network
- Smart Access Gateway
- Data Transfer Plan
- Alibaba Cloud PrivateZone

2.1.11 Database Services

- ApsaraDB for Redis
- ApsaraDB RDS for MySQL
- ApsaraDB RDS for SQL Server
- ApsaraDB RDS for PostgreSQL
- ApsaraDB RDS for PPAS
- ApsaraDB for MongoDB
- ApsaraDB for Memcache
- Data Transmission Service
- AnalyticDB for PostgreSQL
- Distributed Relational Database Service (DRDS)
- Time Series Database (TSDB)
- ApsaraDB for MariaDB TX
- Database Backup
- Data Management
- Data Lake Analytics
- ApsaraDB for POLARDB

2.1.12 Security

- Anti-DDoS Basic
- Anti-DDoS Pro

- Anti-DDoS Premium
- Cloud Firewall
- Web Application Firewall
- Server Guard
- Alibaba Cloud SSL Certificates Service
- Website Threat Inspector
- Managed Security Service
- Content Moderation
- Anti-Bot Service
- Security Center
- GameShield

2.1.13 Monitoring & Management

- CloudMonitor
- Resource Access Management
- Key Management Service
- ActionTrail
- OpenAPI Explorer
- Cloud Shell

2.1.14 Domains & Website

- Web Hosting
- Domains
- Alibaba Cloud DNS

2.1.15 Analytics & Big Data

- E-MapReduce
- MaxCompute
- DataWorks
- Data Integration
- Quick BI
- DataV
- Image Search
- Intelligent Robot
- Dataphin (Coming Soon)
- Machine Learning Platform For AI

- Alibaba Cloud Elasticsearch
- Realtime Compute
- Machine Translation

2.1.16 Application Service

- Message Service
- API Gateway
- Log Service
- Direct Mail
- Blockchain as a Service
- Enterprise Email

2.1.17 Media Services

- ApsaraVideo Live
- ApsaraVideo Media Processing
- ApsaraVideo VOD

2.1.18 Middleware

- Enterprise Distributed Application Service
- Message Queue
- Application Configuration Management
- Tracing Analysis
- Application Real-Time Monitoring Service
- Application High Availability Service
- AliwareMQ for IoT

2.1.19 Cloud Communication

- Short Message Service (SMS)

3 Verification Process - Background

V2.6 of the EU Cloud CoC has been developed against GDPR and hence provides mechanisms as required by Articles 40 and 41 GDPR[6]. Those mechanisms will apply pending the formal approval of the EU Cloud CoC and accreditation of the Monitoring Body.

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679

3.1 Provisional Status of the Verification Process

The services concerned passed a provisional verification process by the Monitoring Body of the EU Cloud CoC, i.e. SCOPE Europe sprl/bvba[7].

This provisional verification process follows the same principles and procedures as the EU Cloud CoC will apply under its official approval and accreditation. The robust and complex procedures and mechanisms can be reviewed by any third party in detail at the website of the EU Cloud CoC alongside a short summary thereof.[8]

3.2 Principles of the Verification Process

Notwithstanding the powers of and requirements set-out by the supervisory authority pursuant Article 41 GDPR, the Monitoring Body will assess whether a Cloud Service, that has been declared adherent to the Code, is compliant with the requirements of the Code - especially as laid down in the Controls Catalogue. Unless otherwise provided by the Code, the Monitoring Body's assessment process will be based on an evidence-based conformity assessment, based on interviews and document reviews; pro-actively performed by the Monitoring Body.

To the extent the Monitoring Body is not satisfied with the evidence provided by a CSP with regards to the Cloud Service to be declared adherent to the Code, the Monitoring Body will request additional information. Where the information provided by the CSP appears to be inconsistent or false, the Monitoring Body will - as necessary - request substantiation by independent reports.

3.3 Multiple Safeguards of Compliance

Compliance of adherent services is safeguarded by the interaction of several mechanisms, i.e. continuous, rigorous and independent monitoring, an independent complaints' handling and finally any CSP declaring services adherent is subject to substantial remedies and penalties in case of any infringement.

3.4 Process in Detail

It is expected that, prior to any assessment of the Monitoring Body, each CSP assesses its compliance internally. When declaring its service(s) adherent to the EU Cloud CoC, each CSP must elaborate its

[7] https://scope-europe.eu
[8] https://eucoc.cloud/en/public-register/assessment-procedure/

compliance with each of the Controls as provided by the Code considering the Control Guidance, as provided by the Control's Catalogue, to the Monitoring Body.

The CSP may do so either by referencing existing third party audits or certifications and their respective reports or by free text. Additionally, the CSP will have to provide a general overview on the functionalities, technical and organizational and contractual frameworks of the service(s) declared adherent.

With regards to internationally recognized standards, the Monitoring Body will consider the mapping as provided by the Controls Catalogue. However, the Monitoring Body will verify whether (a) any third-party certification or audit provided by the CSP applies to the Cloud Service concerned, (b) such third party certification or audit provided by the CSP is valid, (c) such third-party certification or audit has assessed and sufficiently reported compliance with the mapped controls of the third-party certification or audit concerned. Provided that the aforementioned criteria are met, the Monitoring Body may consider such third-party certifications or audits as sufficient evidence for the compliance with the Code.

Within Initial Assessments, the Monitoring Body selects an appropriate share of Controls that will undergo in-depth scrutiny, e.g. by sample-taking and request for further, detailed information including potentially confidential information. Within any other Recurring Assessment, the Monitoring Body will select an appropriate share of Controls provided both that over a due period every Control will be subject to scrutiny by the Monitoring Body and aspects of increased attention as indicated e.g. by media reports, publications and actions of supervisory authorities are covered.

If the responses of the CSP satisfy the Monitoring Body, especially if responses are consistent and of appropriate quality and level of detail, reflecting the requirements of the Controls and indications for appropriate implementation by the Control Guidance, then the Monitoring Body verifies the service(s) declared adherent as compliant and thereupon make them subject to continuous monitoring.

3.4.1 Levels of Compliance

V2.6 of the Code provides three different levels of Compliance. The different levels of compliance relate only to the levels of evidence that are submitted to the Monitoring Body. There is however no difference in terms of which parts of the Code are covered since adherent Cloud Services have to comply with all provisions of the Code and their respective Controls.

3.4.1.1 First Level of Compliance

The CSP has performed an internal review and documented its implemented measures proving compliance with the requirements of the Code with regard to the declared Cloud Service and confirms that the Cloud Service fully complies with the requirements set out in this Code and further specified in the Controls Catalogue. The Monitoring Body verifies that the Cloud Service complies with the Code by information originating from the CSP.

3.4.1.2 Second Level of Compliance

Additional to the "First Level of Compliance", Compliance with the Code is partially supported by independent third-party certificates and audits, which the CSP has undergone with specific relevance to the Cloud Service declared adherent and which were based upon internationally recognised standards procedures. Any such third-party certificates and audits that covered controls similar to this Code, but not less protective, are considered in the verification process of the Monitoring Body. Each third-party certificates and audits that were considered in the verification process by the Monitoring Body shall be referred in the Monitoring Body's report of verification, provided that the findings of such certificates were sufficiently and convincingly reported and documented towards the Monitoring Body and only to the extent such certificates and audits are in line with the Code. The CSP must notify the Monitoring Body if there are any changes to the provided certificates or audits.

The Controls Catalogue may give guidance on third-party certificates and audits that are equivalent to certain Controls in terms providing evidence of complying with the Code.

However, to those Controls that the CSP has not provided any equivalent third-party certificate or audit, the Monitoring Body verifies that the Cloud Service complies with the Code by information originating from the CSP.

The Monitoring Body may refuse application of Second Level of Compliance if third party certificates and audit reports, that are recognized by the Monitoring Body in the verification process concerned, are not covering an adequate share of Controls of this Code; such adequate share shall be subject to the discretion of the Monitoring Body, considering e.g. the share related to the overall amount of Controls of the Code or whether a full Section or topic is being covered.

3.4.1.3 Third Level of Compliance

Identical to the "Second Level of Compliance" but Compliance is fully supported by independent third-party certificates and audits, which the CSP has undergone with regard to the Cloud Service declared adherent and which were based upon internationally recognized standards.

To the extent a CSP refers to individual reports, such as ISAE-3000 reports, the CSP shall ensure that such reports provide sufficient and assessable information and details on the actual measures implemented by the CSP regarding the Cloud Ser-vice concerned. The Monitoring Body shall, if considered necessary, in consultation with the Steering Board, define further requirements on such individual reports, such as accreditation and training for auditors against the provisions and requirements of this Code.

3.5 Transparency about adherence

Each service adherent to the EU Cloud CoC must transparently communicate its adherence by both using the appropriate Compliance Mark[9] and refer to the Public Register of the EU Cloud CoC[10] to enable Customers to verify the validity of adherence.

4 Assessment of declared services by Alibaba Cloud (Singapore) Private Limited (see 2)

4.1 Fact Finding

Following the declaration of adherence of Alibaba Cloud (Singapore) Private Limited ('**Alibaba Cloud**'), the Monitoring Body provided Alibaba Cloud with a template, requesting Alibaba Cloud to detail its compliance with each of the Controls of the EU Cloud CoC. Additionally, the Monitoring Body requested an overview and reasoned response on the actual structure of the services declared adherent and why declared services are to be considered a "service family". A service family requires that all services rely on the same core infrastructure, with regard to hardware and software, and are embedded in the same contractual framework.

Alibaba Cloud promptly responded and extended the template. Information provided consisted of references and list of actual measures meeting the requirements of each Control, a free text answer describing their measures, and a reference to third party audits and certifications, where applicable. Alibaba Cloud provided information illustrating the actual structure of the services declared adherent and describing the technical and contractual framework.

[9] https://eucoc.cloud/en/public-register/levels-of-compliance/
[10] https://eucoc.cloud/en/public-register/

4.2 Selection of Controls for in-depth assessment

Following the provisions of the Code and the Assessment Procedure applicable to the EU Cloud CoC[11], the Monitoring Body analysed the responses and information provided by Alibaba Cloud.

Alibaba Cloud declared services have been externally certified and audited, e.g. Alibaba Cloud holds current SOC 2, ISO 27001 and 27017 certificates. The declaration of adherence referred to the respective ISO 27001 audit report within the responses to Section 6 of the Code (IT-Security). As provided by the Code, the Monitoring Body may consider third party certifications and audits. Accordingly, the Monitoring Body did verify the certification and references. Further in-depth checks were not performed, as provided third party certifications adequately indicate compliance.

First of all the Monitoring Body needed to verify the provided structure and applicability of the role model of one service family. The EU Cloud CoC does not refer explicitly to certain types of Cloud Services; more or less the nature of processing and specifics of Cloud Services – more or less relating to a gradient of responsibilities between CSP and Customer – are the very basis of the Code. However, reference to traditional service types can be a reasonable first indicator. Taking into account the statement of Alibaba Cloud that Cloud Services declared adherent are basically of the type Infrastructure as a Service provided via a platform, the Monitoring Body needed to verify that expectations related to these blueprints are met.

Declared services do not only entail services that are related to the provisions bare metal services. **For the avoidance of doubt**: As the EU Cloud CoC covers the full spectrum of cloud services, responsibility and compliance can be ensured at all time, regardless of the actual categorization of a cloud service.

Another key aspect of the EU Cloud CoC is to ensure that Cloud Service Providers are bound by Customers' instructions and that Cloud Service Providers cooperate with Customers in good faith, including but not limited related to data subject requests. Following the blueprint of IaaS services, it is expected that Customers are enabled to respond data subject requests by themselves, within the technical environment provided by the Alibaba Cloud declared services.

Another area decided to be of relevance for the Initial Assessment has been third country transfers and whether measures regarding safeguards of such transfers are implemented accordingly.

[11] https://eucoc.cloud/en/about/about-eu-cloud-coc/applicable-procedures/

4.3 Examined Controls and related findings by the Monitoring Body

4.3.1 Examined Controls

The Monitoring Body reviewed the initial submission from Alibaba Cloud outlining implemented measures by Alibaba Cloud to meet the requirements of the Code. In line with the Monitoring Body's process outlined in Section 3.4, the Monitoring Body selected a subset of controls from the Code for in-depth scrutiny. The controls selected for this level of review were:

5.1.D, 5.1.E, 5.1.G, 5.2.A, 5.2.B, 5.2.C, 5.2.D, 5.2.H, 5.3.B, 5.3.C, 5.3.D, 5.3.D, 5.4.E, 5.5.C, 5.5.D, 5.7.A, 5.7.C, 5.7.D, 5.7.E, 5.8.A, 5.9.A, 5.9.B, 5.10.A, 5.11.A, 5.11.B, 5.11.C, 5.12.A, 5.12.B, 5.12.C, 5.12.D, 5.12.E, 5.12.F, 5.12.G, 5.12.H, 5.14.C, 5.14.D, 5.14.E, 5.14.F.

Additionally, samples were requested regarding Controls: 5.2.E, 5.3.E, 5.10.B.

Based on the information provided by Alibaba Cloud, a follow-up request was made, for further detail on implemented measures related to Controls and respective information provided for nearly all of the mentioned controls above. **For the avoidance of doubt:** Follow-up questions are not considered as indicator to the quality of first responses; it is expected that in-depth assessments require follow-up requests. Taking into account the high number of Cloud Services subject to this declaration a significant share of follow-up questions was related to verify consistency of measures applicable to all Cloud Services declared adherent. Consequently, follow-up questions were not necessarily related to the response as such but were to a significant share related to the verification of overarching implementation of measures provided.

4.3.2 Findings by the Monitoring Body

During the process of verification, Alibaba Cloud consistently gave impression of having prepared the Declaration of Adherence well and thoroughly. Responses being provided were detailed and never created any impression of intentional non-transparency. Requests for clarification or additional, supporting information and / or evidence were promptly dealt with and always met the deadlines set by the Monitoring Body.

The Monitoring Body did not focus on Section 6, as a current and applicable ISO certification was provided. The Monitoring Body may rely on such external reports and certifications, if those meet the criteria as set out in the Code, which is indicated where such international audit or certification is already being mapped within the Control's Catalogue. Referenced audits and certifications are those international standards, that have been appropriately mapped to Section 6, so that the Monitoring

Body has strong indications allowing the Monitoring Body to rely those. Yet, the Monitoring Body analysed the certifications and assessed whether the scope of applicability covered all Controls as provided by the Code. Regarding the appropriate information security measures according to the sensitivity of the Customer Personal Data, Alibaba Cloud provided convincing responses, indicating that the implemented information security measures always relate to the potentially highest risks concerned and that there is no discriminate in measures depending on Customers and / or related Customer Personal Data. The latter is of highest relevance as Alibaba Cloud is not fully aware of the actual data that is being processed by Customers as consequence to the design of the Cloud Services.

Considering the amount of Cloud Services declared adherent the Monitoring Body spent a significant share of its assessment in verifying that Cloud Services declared adherent are one service family. **For the avoidance of doubt:** The Monitoring Body did not assess any Cloud Service individually. It assessed the overall procedures and structures and verified if provided responses are consistent. Therefore, Monitoring Body verified several aspects by taking samples. Those samples were not related to individual controls but were related to the information provided publicly to each Cloud Service and whether such information is consistent with the information provided during the assessment. The Monitoring Body took several examples. Whilst in general the responses and publicly available information was consistent, there were individual findings that first appeared as inconsistencies. The Monitoring Body referred to Alibaba Cloud and requested explanation. Alibaba Cloud promptly provided convincing responses resolving any inconsistencies. **For the avoidance of doubt:** To the understanding of the Monitoring Body publicly available documentation can be modified by Customers as such documentation seems to follow a WIKI-alike approach based on GitHub. Consequently, publicly available language may easily slightly differ from language originating from the CSP itself. Thus, such areas of possible inconsistencies are no indicator of intent.

The Monitoring Body also verified, based on samples, information provided by Alibaba Cloud that retrieval of Customer Personal Data is possible at all times and Customer may access related information upfront, e.g. by reading Cloud Service specific API-Documentation. Samples taken by the Monitoring Body verified that such API-Documentation is being provided and that such API-Documentation includes information how to retrieve data but also that Customer may configure the Cloud Service via API-accordingly that may also amount to Instructions in the meaning of GDPR.

The overall impression whilst assessing Alibaba Cloud was positive. Alibaba Cloud referred to applicable policies and procedures. Main reference and source of implemented controls was the Security

Whitepaper in version 2.0, 2020.[12] The Whitepaper has been subject to updates during the process of assessment which has been rewarded by the Monitoring Body as evidence that implemented technical and organisational measures are subject to constant evaluation.

Regarding the requirements of assisting Customers, due to the nature of the service environment, compliance with all respective Controls was expected by fully enabling Customers, e.g. to respond data subject requests. Alibaba Cloud provided adequate information that Customers are fully enabled to respond to data subject requests by themselves, without any needs of additional support by Alibaba Cloud. However, Alibaba provides several communication channels, by which Customers may reach out in case they need further assistance, e.g. via customer dashboard, can contact or instruct Alibaba Cloud in line with Code requirements. **For the avoidance of doubt:** Depending on the individual configuration applied by Customers further assistance may be limited, as even Alibaba Cloud has not any access to Customer Personal Data concerned.

Regarding the technical and organizational measures in general, the nature of processing also requires that Customers are fully enabled to implement appropriate measures. Shared responsibilities of CSP and Customer are transparently communicated by several documents, i.e. the Cloud Service Agreement, but also documentation related to each Cloud Service – e.g. configuration manuals, best practise, API-Documentation, but also within the Security Whitepaper and the Security & Compliance Centre.

Regarding mechanism whereby the Customer shall be notified of any changes concerning an addition or a replacement of a subprocessor, Alibaba Cloud provides reasonable prior notification. However, as stated by Alibaba Cloud, there are currently no subprocessors. Responses provided were consistent from a procedural perspective. However, a more consistent language regarding subprocessors and subcontractors would be welcomed. It is also highly appreciated that Alibaba Cloud is willing to address individual Customer inquiries by agreeing upon additional measures treating non-subprocessors equally to subprocessors under GDPR.

In summary, the provided information by Alibaba Cloud was convincing and the Monitoring Body found no indications for intentional non-transparency. **For the avoidance of doubt**: As a large number of services were declared adherent, the Monitoring Body did not assess all services in-depth. As all declared services rely on the same core infrastructure, with regard to hardware and software, and

12 https://resource.alibabacloud.com/whitepaper/alibaba-cloud-security-whitepaper---international-edition-v20-2020_1717?spm=a3c0i.8119595.5143247140.2.4f60411diUnMdW

are embedded in the same contractual framework, the Monitoring Body found no clear evidence why some services should not be in line with the findings as outlined. However, further samples of individual services can be subject of future renewals of the declaration of adherence.

5 Conclusion

Given answers by Alibaba Cloud were consistent. Where necessary Alibaba Cloud gave additional information or clarified their given information appropriately.

The Monitoring Body therefore verifies the services as compliant with the EU Cloud CoC based on the performed assessment as prescribed in 1. The service(s) will be listed in the Public Register of the EU Cloud CoC[13] alongside this report.

[13] https://eucoc.cloud/en/public-register/

6 Validity

This verification is valid for one year. The full report consists of 18 pages in total, whereof this is the last page closing with the Verification-ID. Please refer to the table of contents at the top of this report to verify, that the copy you are reading is complete, if you have not received the copy of this report via the Public Register of the EU Cloud CoC[14].

Verification-date: June 2020 **Valid thru**: June 2021

Verification-ID: 2020PV02SCOPE013

[14] https://eucoc.cloud/en/public-register/